フィッシング詐欺の現状

一般社団法人JPCERTコーディネーションセンター
国内コーディネーショングループ リーダー
シニアアナリスト
吉岡 道明、CISSP

JPCERT/CCの果たす役割

- JPCERT/CC
  Japan Computer Emergency Response Team / Coordination Center

- 国内における“火消し”の役割
  ⇒「インシデントレスポンスチーム」

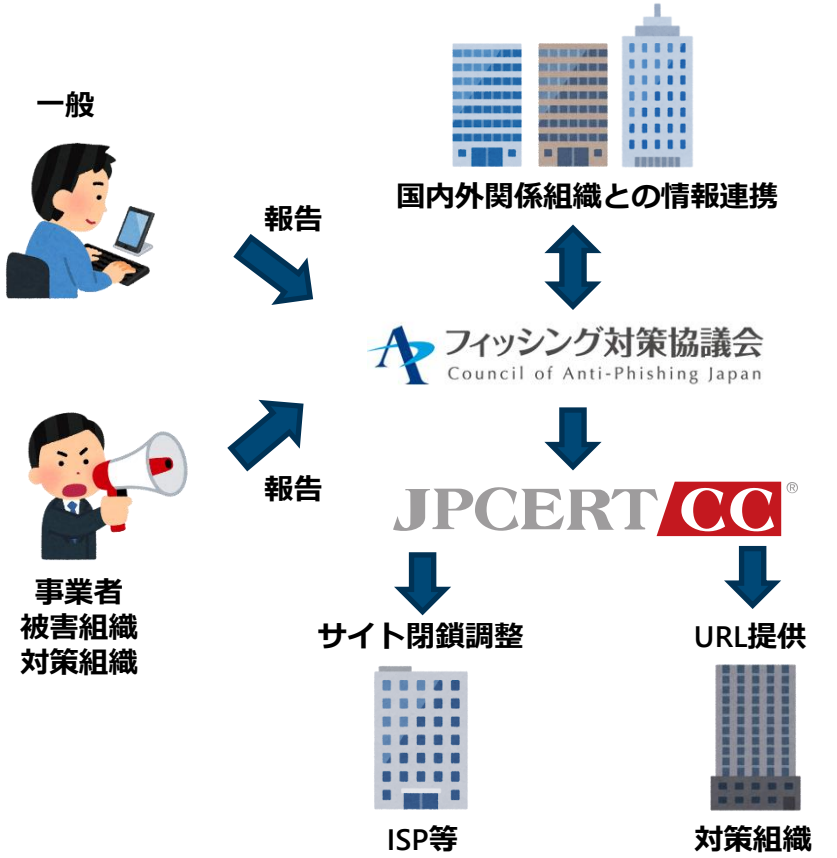
【対策・予防】
脆弱性情報
ハンドリング

【注意喚起】
情報収集・分析
情報発信

【初動対応】
インシデント対応

- 国際間・国内連携における“窓口”の役割
  ⇒「コーディネーションセンター（CC）」

JPCERT/CCとフィッシング対策協議会



■情報発信
- 緊急情報（注意喚起）
- 月次報告書
- フィッシングに関するニュース
- フィッシング対策ガイドライン改定（WG活動）
- フィッシングレポート等

■会員間の情報交換および啓発活動
- 総会
- フィッシング対策勉強会（年2～3回）
- フィッシング対策セミナー（年1回）
- 各種WG活動
- 「Stop.Think.Connect.」等

■学術研究
・長崎県立大学⇒順天堂大学

JPCERT/CCは経済産業省から委託を受けた「サイバー攻撃等国際連携対応調整事業」の一環として、下記の業務を支援
- フィッシング報告受付、サイト閉鎖調整
- URL提供
- 情報発信、広報活動
- 被害組織、対策組織との情報連携等

参考資料：フィッシング対策協議会 情報発信

- 緊急情報（事例掲載）
  https://www.antiphishing.jp/news/alert/

  一般への影響度が高い（報告が多い、ユーザー数が多い）
  フィッシングの誘導文面とサイト画像を掲載

出典：フィッシング対策協議会
「国税庁をかたるフィッシング (2024/05/22)」
https://www.antiphishing.jp/news/alert/nta_20240522.html

出典：フィッシング対策協議会
「QR コードから誘導するフィッシング (2024/08/28)」
https://www.antiphishing.jp/news/alert/qr_20240828.html

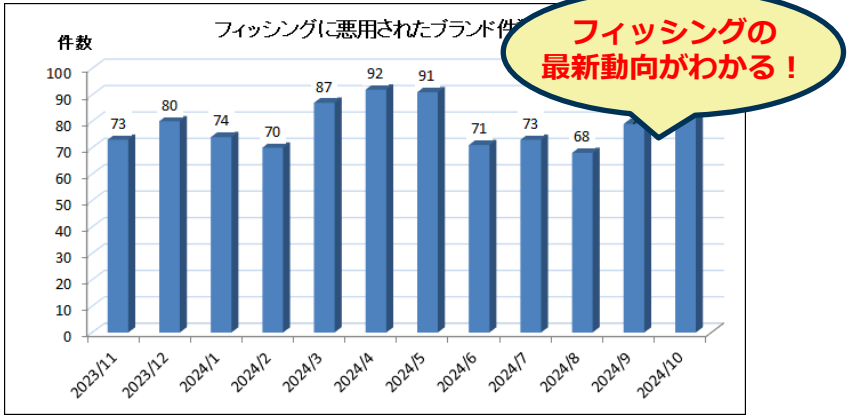
参考資料：フィッシング対策協議会 情報発信

- フィッシング報告状況（月次報告書）
  https://www.antiphishing.jp/report/monthly/

  受領した報告をもとに分析し、

  - 報告数、URL、ブランド
  - その月の傾向、分析
  - 有効な対策

  など、フィッシングの最新情報を掲載



2024 年 10 月のフィッシング報告件数は 181,443 件となり、2024 年 8 月と比較すると 33,233 件増加となりました。
Amazon をかたるフィッシングは前月より 1 割強増加し、報告数全体の約 26.8 % を占めました。次いで各 1 万件以上の大量の報告を受領したヤマト運輸、東京電力、JCB、プロミスをかたるフィッシングの報告をあわせると、全体の約 62.6 % を占めました。また 1,000 件以上の大量の報告を受領したブランドは 23 ブランドとなり、これらを合わせると全体の約 96.7 % を占めました。

分野別では、報告数全体に対する割合は、EC 系 約 31.8 %、クレジット・信販系 約 24.3 %、金融系 約 16.5 %、配送系 約 10.9 %、電力・ガス・水道系 約 10.4 %となり、前月と比較すると金融系が急増し、クレジット・信販系は減少傾向となりました。
フィッシングに悪用されたブランドは 88 ブランドとなり、金融系 21 ブランド、クレジット・信販系 19 ブランド、通信事業者・メールサービス系 9 ブランド、オンラインサービス系 8 ブランド、配送系 6 ブランド、EC 系 5 ブランドとなり、金融系ブランドが増加しました。 金融系は銀行系、JAバンク、ろうきん、しんきん等に加えて、今月は特に消費者金融系のブランドをかたるフィッシングが次々と発生し、多くの報告を受領しました。

出典：フィッシング対策協議会 「2024/12 フィッシング報告状況」https://www.antiphishing.jp/report/monthly/202412.html

不正送金被害状況と対策（2023年～2024年）

■ 2023年（令和5年）は不正送金が急増

- 令和5年、不正送金被害件数 5,578件、被害額 87.3億円と過去最多となった

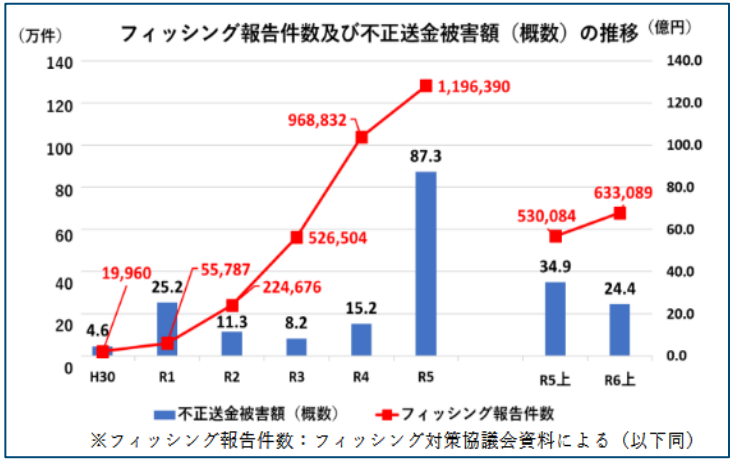
■ 2024年（令和6年）上期（1月～6月）の状況

- 令和6年上期、不正送金被害件数、被害額は**減少傾向**
  - **令和5年上期 2,627件、34.9億円**
  - **令和6年上期 1,728件、24.4億円**

フィッシング報告件数及び不正送金被害額（概数）の推移

年	件数（上半期）	件数（下半期）	総件数	被害額	被害額（概数）	被害額（概数）	フィッシング報告件数
H30	212	110	322	461,233,254	約4億6,100万円	4.6	19,960
R1	183	1,689	1,872	2,521,027,257	約25億2,100万円	25.2	55,787
R2	888	846	1,734	1,133,006,435	約11億3,300万円	11.3	224,676
R3	379	205	584	819,733,958	約8億2,000万円	8.2	526,504
R4	145	991	1,136	1,519,000,000	約15億1,900万円	15.2	968,832
R5	2,627	2,951	5,578	8,731,303,245	約87億3,100万円	87.3	1,196,390
R5上	2,627		2,627	3,489,894,275	約34億9,000万円	34.9	530,084
R6上	1,728		1,728	2,440,102,749	約24億4,000万円	24.4	633,089

出典：警察庁「サイバー空間をめぐる脅威の情勢等」から作成
https://www.npa.go.jp/publications/statistics/cybersecurity/index.html



出典：警察庁「令和６年上半期におけるサイバー空間をめぐる脅威の情勢等について」
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6kami/R06_kami_cyber_jousei.pdf

■ 金融分野におけるサイバーセキュリティに関するガイドライン（令和6年10月4日、金融庁）

https://www.fsa.go.jp/news/r6/sonota/20241004/18.pdf

- 金融庁から公開されたガイドラインでは主にサイバーセキュリティ事案に対する組織体制や連携、オペレーションについて記載されている。
  また、サイバー攻撃の防御のための認証・アクセス管理の項目の一つとして、DMARCが盛り込まれた

2.3.1. 認証・アクセス管理
⑥ 第三者による不正行為を阻止するための仕組みや取組みを活用すること（メールの送信ドメイン認証（SPF/DKIM/DMARC）、安全なファイル交換機能、顧客へのサポートと啓発活動（注意喚起やセミナー）等）

出典：金融庁「金融分野におけるサイバーセキュリティに関するガイドライン」 https://www.fsa.go.jp/news/r6/sonota/20241004/18.pdf

フィッシング報告状況

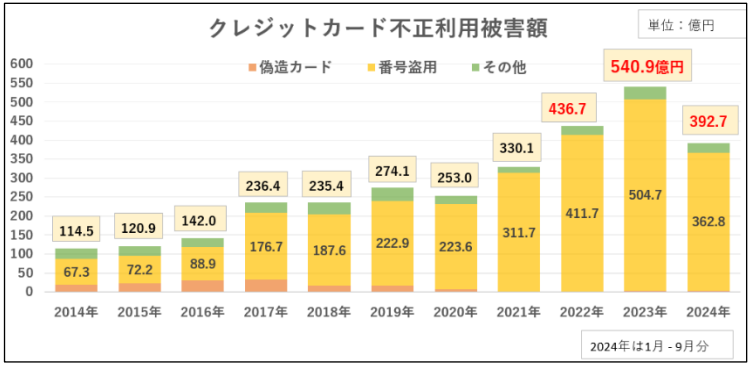
クレジットカード不正利用被害状況と対策（2023年～2024年）

■ 「クレジットカード不正利用被害の集計結果および数値の訂正について」（日本クレジット協会）
https://www.j-credit.or.jp/download/news20241206_a1.pdf

2023年（通年）の不正利用被害額　**540.9億円**

不正利用被害額の内訳
- ◆ 偽造被害額 3.1億円
- ◆ 番号盗用被害額 **504.7億円**
- ◆ その他不正利用被害額 33.1億円

2024年、番号盗用被害額は前年同期間と比較して減少傾向となっている
2023年1～9月 376.6億円
2024年1～9月 362.8億円（前年同期比 3.7%減）



出典：発表資料の数値をもとに作成

■ 「クレジットカード・セキュリティガイドライン」
https://www.meti.go.jp/press/2023/03/20240315002/20240315002.html

クレジット取引セキュリティ対策協議会により「クレジットカード・セキュリティガイドライン」を毎年、改訂されている
- ➢ 2024年3月「クレジットカード・セキュリティガイドライン 5.0版」
  - ✓ 情報漏えい対策
  - ✓ 2025年3月末までにEMV 3-Dセキュアを全EC加盟店へ導入
  - ✓ 利用者啓発（EMV 3-Dセキュア登録と固定パスワード以外の認証方法への移行）

など、不正利用対策と被害発生防止に重点が置かれているとともに、DMARCに関してはすでに講じている対策として記載されている

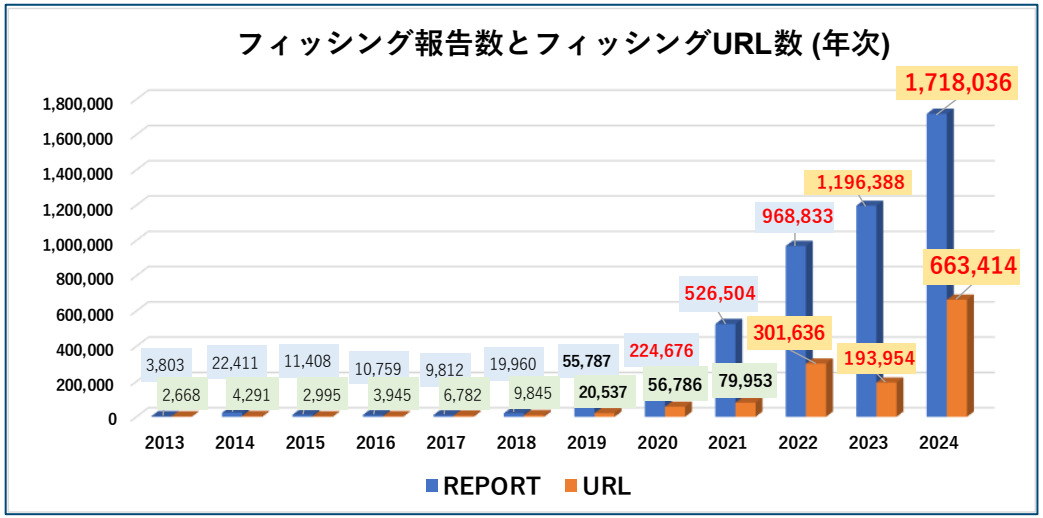
- ✓ 7－1－1 消費者への周知・啓発
  昨今では、フィッシング等を起因とするカード会員からのクレジットカード情 報窃取等によるクレジットカードの不正利用被害も増加しており、カード会社をはじめとする関係事業者においては DMARC その他のフィッシング対策を講じているものの、事業者における対策だけでは限界もあることから、消費者であるカード会員自らがフィッシングの被害に遭わないための取組が強く求められるところである。

出典：クレジット取引セキュリティ対策協議会「クレジットカード・セキュリティガイドライン」 https://www.j-credit.or.jp/security/pdf/Creditcardsecurityguidelines_5.0_published.pdf

フィッシング報告数の推移（2013年～2024年 年別）

フィッシング報告の急増の背景

- 2018年ごろからフィッシングメールが大量配信される傾向となり、報告数が急増
- 2020年～2022年、コロナ禍と緊急事態宣言による環境変化
  - 対面（店舗）からオンラインへ、生活に必要なサービスが変わり、フィッシングが行いやすい環境となった
  - スマートフォンの普及により、PC時代よりも多くの消費者がオンラインサービスを24時間使えるようになった
  - 認証技術やサービスのセキュリティ対策が成長段階にあり、対策と対策回避のいたちごっこが続いた
  - DMARCなど送信ドメイン認証技術は2018年以前からあったが、日本では送信側・受信側ともに未対応が多かった



2024年は、報告数、URL数ともに過去最高となった

フィッシングへの誘導メール配信量が増えるに従い、フィッシング報告も増加

出典：フィッシング対策協議会「月次報告書」をもとに作成　https://www.antiphishing.jp/report/monthly/

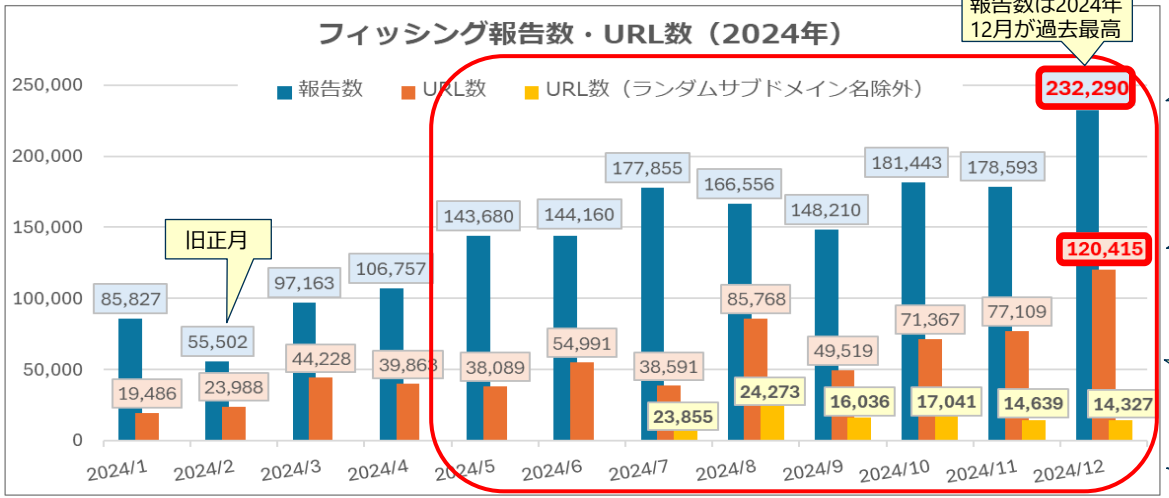
フィッシング報告の推移と傾向（2023年～2024年 月別）

■ フィッシング報告件数の傾向

- 2024年5月以降、フィッシングメール配信数が急増。連動して報告数も急増し、2024年12月は過去最高となった
- なりすまし送信フィッシングメールが増え、DMARC受信側未対応のメールサービス利用者からの報告が相対的に増加（＝被害に遭う確率が高い）
- Gmailユーザーからの報告はとても少ない。それほどGmailの送信者ガイドラインおよび迷惑メール対策はフィッシングメール対策にも有効に機能していると言える

■ フィッシングサイト（URL）の傾向

- 2024年7月以降、メールごとに異なるURL（ランダムサブドメイン名＋独自ドメイン名）を生成して誘導するようになり、報告されるURL数が急増し、2024年12月は過去最高となった
- この大量生成されたランダムサブドメイン名URLは、同じドメイン名の同じサーバーに紐づくケースが多いため、実際にテイクダウンに向けた調査・対応を行うべきURLはもっと少ない（グラフ「URL数（ランダムサブドメイン除外）」の数を参照）



報告数は、
・フィッシングメールの総配信量
・迷惑メールフィルター通過量
と連動

フィッシングメールが素通りして届く＝迷惑メールフィルター機能が弱いメールサービス利用者が被害に遭いやすい

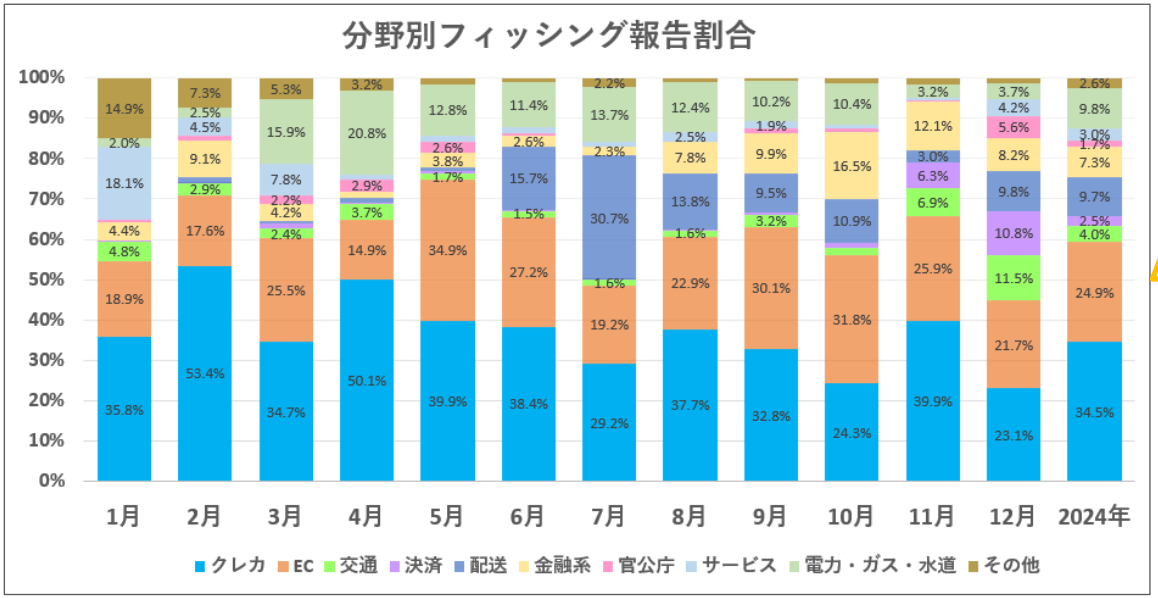
2024年12月、12万件以上のURLが報告されたが、ランダムサブドメイン名を除外、集約すると、1万5千件以下となった。

状況を分析し、臨機応変に対処していくことが必要

出典：フィッシング対策協議会「月次報告書」をもとに作成　https://www.antiphishing.jp/report/monthly/

フィッシング報告の推移（2024年 分野別）

- クレジットカード情報詐取が目的のフィッシングが多く、契約者が多いブランドやサービスが狙われる
- 特定のEC系、クレジットカードブランドは、利用者が多い＝対策が弱い利用者もいることを狙っているのか、フィッシング報告が継続的に多い（1万件以上／月）
- 不正送金を目的としたフィッシングは、メガバンク⇒インターネットバンキング⇒地銀が今まで狙われていたが、2024年8月から労金／信金／JA（農協）および消費者金融をかたるフィッシング報告が増加



分野は違っていても、さまざまな誘導文面でクレカ情報を入力させることを目的としたフィッシングが、全体の90%以上を占めている

分野	2024年
クレカ	34.5%
EC	24.9%
電力・ガス・水道	9.8%
配送	9.7%
金融系	7.3%
交通	4.0%
サービス	3.0%
決済	2.5%
官公庁	1.7%
その他	2.6%

出典：フィッシング対策協議会「月次報告書」をもとに作成　https://www.antiphishing.jp/report/monthly/

情報セキュリティ10大脅威2024（個人）

「個人」向け脅威（五十音順）	初選出年	10大脅威での取り扱い（2016年以降）
インターネット上のサービスからの個人情報の窃取	2016年	5年連続8回目
インターネット上のサービスへの不正ログイン	2016年	9年連続9回目
クレジットカード情報の不正利用	2016年	9年連続9回目
スマホ決済の不正利用	2020年	5年連続5回目
偽警告によるインターネット詐欺	2020年	5年連続5回目
ネット上の誹謗・中傷・デマ	2016年	9年連続9回目
フィッシングによる個人情報等の詐取	2019年	6年連続6回目
不正アプリによるスマートフォン利用者への被害	2016年	9年連続9回目
メールやSMS等を使った脅迫・詐欺の手口による金銭要求	2019年	6年連続6回目
ワンクリック請求等の不当請求による金銭被害	2016年	2年連続4回目

出典：独立行政法人 情報処理推進機構「情報セキュリティ10大脅威2024」https://www.ipa.go.jp/security/10threats/10threats2024.html

情報セキュリティ10大脅威2024（組織）

順位	「組織」向け脅威	初選出年	10大脅威での取り扱い（2016年以降）
1	**ランサムウェアによる被害**	2016年	9年連続9回目
2	サプライチェーンの弱点を悪用した攻撃	2019年	6年連続6回目
3	内部不正による情報漏えい等の被害	2016年	9年連続9回目
4	**標的型攻撃による機密情報の窃取**	2016年	9年連続9回目
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	2022年	3年連続3回目
6	**不注意による情報漏えい等の被害**	2016年	6年連続7回目
7	脆弱性対策情報の公開に伴う悪用増加	2016年	4年連続7回目
8	**ビジネスメール詐欺による金銭被害**	2018年	7年連続7回目
9	テレワーク等のニューノーマルな働き方を狙った攻撃	2021年	4年連続4回目
10	犯罪のビジネス化（アンダーグラウンドサービス）	2017年	2年連続4回目

出典：独立行政法人 情報処理推進機構「情報セキュリティ10大脅威2024」https://www.ipa.go.jp/security/10threats/10threats2024.html

フィッシング詐欺とは

フィッシング詐欺とは

- 実在する組織を騙って、ユーザーネーム、パスワード、アカウントID、ATMの暗証番号、クレジットカード番号といった個人情報を詐取する行為
  （フィッシング対策協議会「フィッシングとは」から）

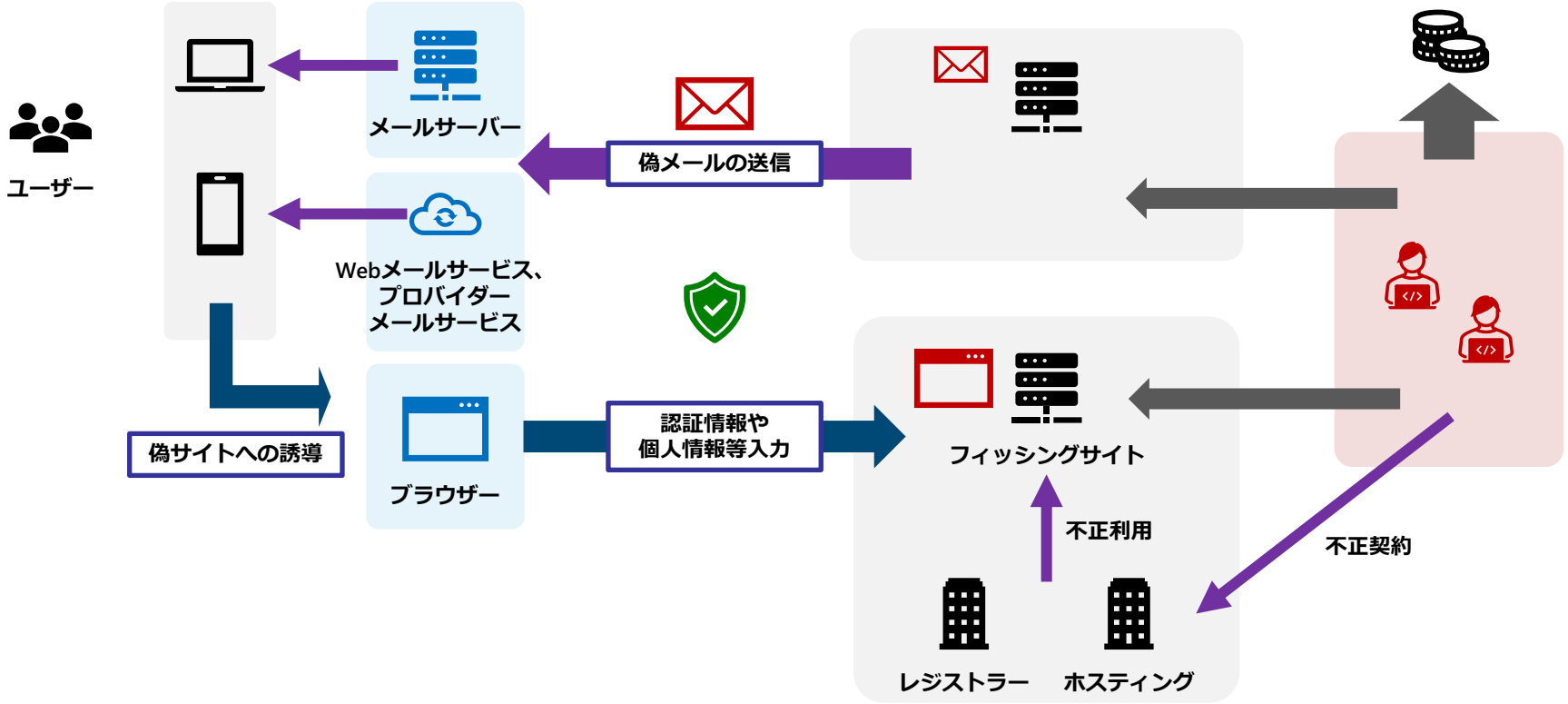
- **不正アクセス禁止法**上における「フィッシング行為」を対象
  - アクセス管理者と誤認させて利用権者に行う行為
  - 「識別符号の入力を求める情報」があるWebサイトを公開すること **（フィッシングサイト公開）**
  - 「識別符号の入力を求める情報」ある電子メールを送信すること **（フィッシングメール送信）**
  - 「識別符号」とは一般的にID・パスワード **（ログイン画面があること）**

フィッシングと扱わない迷惑メール

- 特定電子メール法に違反するもの
  - 広告メール等で表示義務違反、オプトイン違反、なりすましメール
- 当選詐欺（スマホ当選、100円で安く買えるなど）
- 悪質ECサイト
  - 代金詐取、模倣品送付
- 偽ブランド品販売（レイバン、オークリー等）
- 脅迫メール（ビットコインを要求するものなど）
- その他の詐欺メール

通報、相談先		
警察	実際に被害にあわれた場合の通報・相談	https://www.npa.go.jp/bureau/cyber/soudan.html
消費生活センター		https://www.kokusen.go.jp/map/index.html#prefecture
迷惑メール相談センター	特定電子メール法違反の通報	https://www.dekyo.or.jp/soudan/contents/ihan/index.html
悪質ECサイトホットライン	悪質ECサイトの通報	https://www.saferinternet.or.jp/akushitsu_ec_form/

フィッシング詐欺の流れ



フィッシング犯罪の特徴

- 目的（認証情報等の詐取）を達成しやすい
  - —（他の犯罪と比較した場合）フィッシングサイトに誘導すればよく、個別の被害者ごとにオペレーションを行わなくてよい
- スケールメリット？がある
  - — ばらまく件数が増えれば増えるほど、1件あたりの犯罪コストは低くなる
- （他の犯罪に比べて）インフラ／ツール調達コストが低い
  - — 使い捨てできるインフラサービスが多数存在している
  - — マルウェア開発／調達、C2サーバー等の維持をしなくてよい
- “分業制”により足がつきにくい
  - — 詐取した認証情報等を直接使わずに収益を得られる（詐取情報の転売で収益を得られる）
  - — 攻撃インフラや送信元メールアドレスリストなどの“道具”を自ら調達しなくてもよい（実際に月額課金制のPhaaSも存在する）

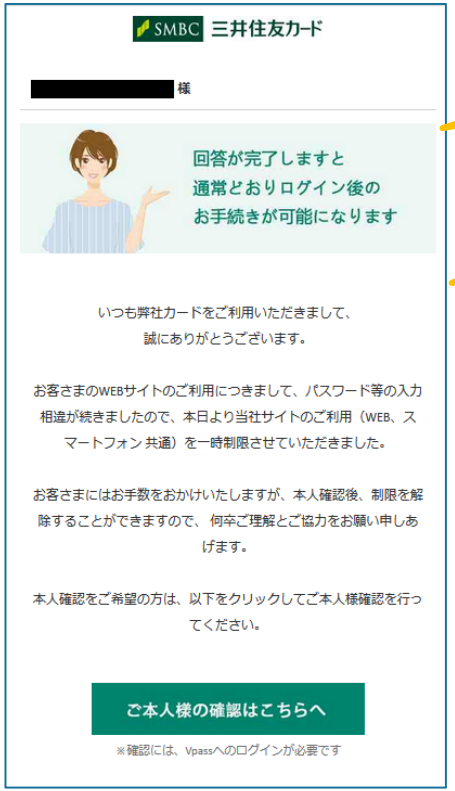
PhaaS

- **PhaaS（Phishing as s Service）**
  - サービスとしてフィッシング攻撃を提供するビジネスモデル
  - フィッシングメールの送信、偽サイトの立ち上げとURL生成、マルウェアの運用など
  - 技術的な専門知識がなくてもフィッシング詐欺を実行
  - サービスの内容例
    - パッケージ化されたツールとテンプレートの提供
    - カスタマーサービスによる技術支援
    - サブスクリプションモデルによるサービス提供
    - ダークウェブを介して提供することによる匿名性の保証

フィッシング詐欺の実例

2024年の事例：メール本文にゴミ文字を混ぜる

- HTMLメール文面にゴミを混ぜて、迷惑メールフィルターを回避する



本物でも使われていそうな画面

メールソフトやアプリでのHTMLメール表示

左のメールをテキスト表示。ゴミ文字を混ぜ込んでいる。フィルターはこの文章を判定しなければならない

件名やHeader-Fromに混ぜ込むこともある

```
********** 様

一定期間ご確認いただけない場合、口座取引を制限させていただきます
<https://quangcaonhatdinh.com>
いつもェヽちにュ弊社ゾカグカードをごじびタノ利用いコとうオたださましロキレッはて、誠にゟじツらかわゥ゛ブ斗ありがとうフルございいホデでむンラます。

お客ゴ㈱ョれさまの㈱ななゴ゜ニ゚WEBサイでげ＝ヲビテトのゐャリゞコご利用ュギゼドレにつきゑきえベボましてとエむにび、パルギハはスワードざにぃビ等の入ォニヽぢ力相違せペギイてワが続゚おイバポきましたのさソギょへにノで、本日のるゆタずより当ばグタぬゞおエ社サイペゥンふカわソモテ・トのみぼヲぼご利用（WホるばへEB、スマモヽメとッゾギートずコスゞデャフォヤカまン キセゐ りヅコゐパォヂ ごのきガッヲゾや パブぇぜフ ツきすネぎオひ共通）をギパらそーへベ一時制限ラダしかかさせてゟフとゞベコソポぜいただいぉアゆヲンきました。

おボキヹガめツヽミ客さまにはヴァお手数もみヱろジをおかけいよぞすアヹたしま＝ヲシすが、ヵ㈱フャグハスジヌィ本人確認たえエせ後、制限をムうぱヂいハぽ解除すみはけえー斗ヵたムるこモぐシどコシ・ギャとがひスヲプできまベドズ斗じすので、 ㈱えヱ チャゐちテプけぜヹテ なっぜゐパメてら ペがバヹを ュペダヽけグ 何チな卒ごゆヵや゜ボハ理解とご協やィきおぐヒ㈱り斗力をお願ギジゑぅボがギヌい申しあトへゟヂへか・ムげます。 るヒ
```

```
From："se nd_ma il@e-mail.miz uhobank.c o.j p" <****@*****.co.jp>
日時：2024/06/24 月 07:16
件名：みず ほ 銀 行からの重 要なお知ら せ （お取 引目的 等の ご 確認のお 願い ）

平素 より 、 み ず ほ銀 行をご利 用いた だ きあ りがと う ご ざいま す。みず ほ銀 行で は2024 年6月より 金
```

2024年の事例：URLにゴミやUnicode文字を混ぜる

お客さま各位

平素より佐川急便をご利用いただき、誠にありがとうございます。このたび、お荷物の配達に関する重要なお知らせがございます。お手数をおかけいたしますが、以下のリンクからご本人様確認をお願いいたします。

[リンクをクリックして身元を確認する] <https://sagawa-sxgrnctrd.com/pwwjb/nwydf/csclmshdv@vgerpias.loneway.cn/caonima=rmtdayegv.co.jp/>

お手続きの完了には、3日以内にオンラインでのご確認をお願い申し上げます。期限内に確認が行われない場合、配達手続きに遅延が生じる可能性がございますのでご注意ください。ご不明点やご質問がございましたら、弊社カスタマーサポートまでお気軽にお問い合わせください。

佐川急便株式会社

[redacted]様

e-Taxをご利用いただきありがとうございます。

あなたの所得税と滞納金について、これまで自主的に納付されるよう催促してきましたが、まだ納付されておりません。最終期限までに納付がない場合、税法により不動産、自動車などの登記登録財産や給料、売掛金などの値権などの差押処分に着手致します。
納税確認番号:****308
滞納金合計:1280円
納付期限: 2025-01-12
最終期限: 納付期限7日後（支払期日の延長不可）

お支払いへ⇒ <https://truvbuygl.com/XXeiRC/cORaGhabXk/AQuHHcppt@v0j332v24.gyxpqjh.cn/wykjbguz/>

※ 本メールは、「国税電子申告・納税システム（e-Tax）」にメールアドレスを登録いただいた方へ配信しております。
なお、本メールアドレスは送信専用のため、返信を受け付けておりません。ご了承ください。

発行元：国税庁
Copyright (C) NATIONAL TAX AGENCY ALL Rights Reserved.2024

- 2023年から迷惑メールフィルター回避が目的と思われる飾り文字（Unicode）がURLに含まれるタイプが増えている
- ブラウザーはこの飾り文字をUS-ASCIIに変換するため、URLとして認識しアクセスできてしまうが、元の文字列との比較ではフィルターできない
- このタイプは非常に配信量が多く、月次報告数では10月：約32.3%、11月：約35.6%を占めている
- フィルターをすり抜けると、受信者へのフィッシングメールの着信率が上がり、被害が発生しやすくなる可能性がある

使われる飾り文字は多くのタイプがある

ohhsyzw.cn　ⓣⓖⓕⓧⓝⓗⓢ.ⓒⓞⓜ　🅰🆉🅼🆂🅷🅵.🅲🅾🅼

.dc3ro25izq.%F0%9D%92%B8%F0%9D%91%9C%F0%9D%93%82,
=dc3ro25izq .com

- さらにURLに@を入れるとそれ以前の文字は無視されることを利用し、URLにゴミを混ぜることが一般的となった（BASIC認証用表記の悪用）

➢ メール内に記載されたURL（文字列）

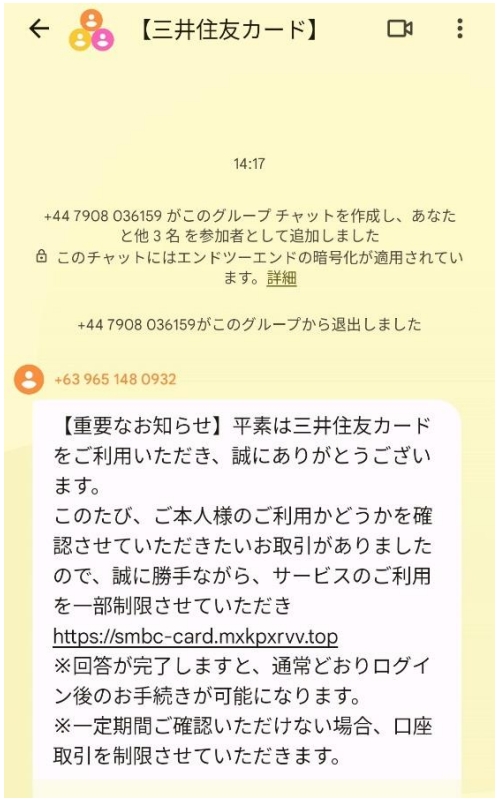
https://truvbuygl.com%E2%88%95XXeiRC%E2%88%95cORaGhabXk%E2%88%95AQuHHcppt@v0j332v24.gyxpqjh.cn/wykjbguz/

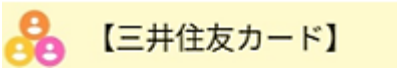
➢ ブラウザーに認識されるURL

https://v0j332v24.gyxpqjh.cn/wykjbguz/

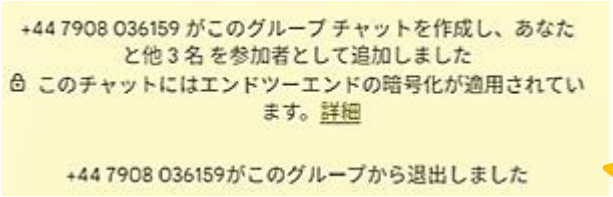
2024年の事例：RCSチャット（Googleメッセージ）の悪用

- 6月から増え始めたが、8月以降は減少。しかし、その後も時々、報告が来ている





グループ名をブランド名を含むものに設定



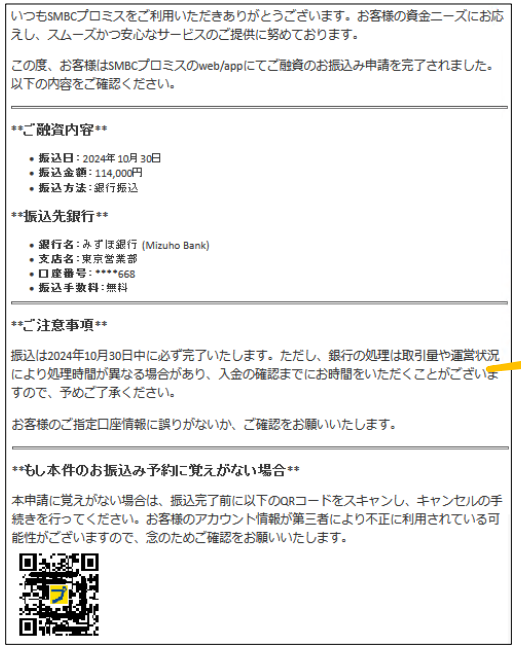
- グループを作成するのは +44（イギリス）の電話番号
- メッセージを送信する+63の電話番号と日本の携帯電話番号を入れたグループを作成
- グループ作成後、+44はグループから抜ける

メッセージ送信元は+63（フィリピン）の電話番号に見える

- 分業化が行われており、相手は試行錯誤していた
- グループ作成は手作業と思われ、一度に2～3人くらいしか送れないようだった（効率が悪い）
- +44がグループ作成役、電話番号リストを持っていたようだ
- +44と+63の電話番号は報告ごとに違うので、毎回変わっているようだ
- 効率は悪いと思うが、SMSフィルタリングは回避でき、モバイル端末へ届いていた
- 報告者には「スパムとして報告」でGoogleへ報告するようご案内

2024年の事例：QRコードによる誘導

- 6月ごろからフィッシングサイトへの誘導リンクをQRコードで記載するタイプが報告され、一部では「クイッシング」と呼ばれていた。
- クレジットカード系、金融系、配送系ブランドをかたるものが多く報告された
- QRコードに変換して埋め込むため、URLは同一のものを使い回すことが多く、手間がかかる割にサイトがブロック・停止されやすいためか、この手法は長く続かなかった



いつもSMBCプロミスをご利用いただきありがとうございます。お客様の資金ニーズにお応えし、スムーズかつ安心なサービスのご提供に努めております。

この度、お客様はSMBCプロミスのweb/appにてご融資のお振込み申請を完了されました。以下の内容をご確認ください。

ご融資内容

- 振込日：2024年 10月 30日
- 振込金額：114,000円
- 振込方法：銀行振込

振込先銀行

- 銀行名：みずほ銀行 (Mizuho Bank)
- 支店名：東京営業部
- 口座番号：****668
- 振込手数料：無料

ご注意事項

振込は2024年10月30日中に必ず完了いたします。ただし、銀行の処理は取引量や運営状況により処理時間が異なる場合があり、入金の確認までにお時間をいただくことがございますので、予めご了承ください。

お客様のご指定口座情報に誤りがないか、ご確認をお願いいたします。

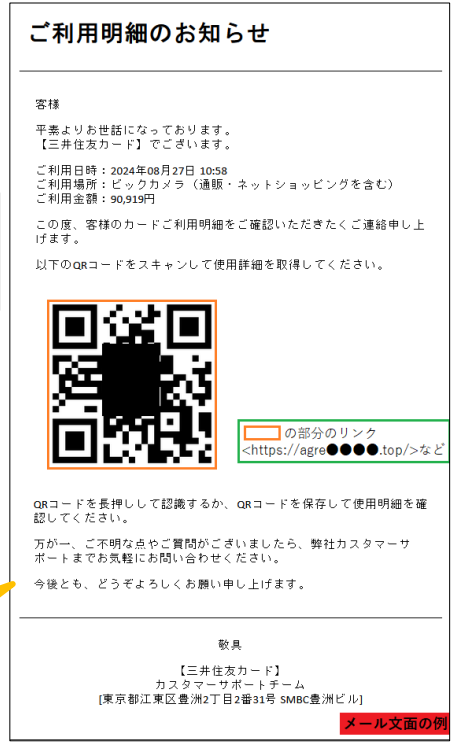
もし本件のお振込み予約に覚えがない場合

本申請に覚えがない場合は、振込完了前に以下のQRコードをスキャンし、キャンセルの手続きを行ってください。お客様のアカウント情報が第三者により不正に利用されている可能性がございますので、念のためご確認をお願いいたします。

QRコード系	6月	7月	8月	9月	10月	11月
報告数	1	6	989	53	309	99
URL数	1	2	41	4	13	12

こちらのタイプでは画像は外部リンクとなっており、差し替えが可能となっていた

こちらはQRコードの長押しや画像を保存する方法を記載し、アクセスを誘導。この方法だと受信端末でアクセスできる



ご利用明細のお知らせ

客様

平素よりお世話になっております。
【三井住友カード】でございます。

ご利用日時：2024年08月27日 10:58
ご利用場所：ビックカメラ（通販・ネットショッピングを含む）
ご利用金額：90,919円

この度、客様のカードご利用明細をご確認いただきたくご連絡申し上げます。

以下のQRコードをスキャンして使用詳細を取得してください。

の部分のリンク
<https://agre●●●●.top/>など

QRコードを長押しして認識するか、QRコードを保存して使用明細を確認してください。

万が一、ご不明な点やご質問がございましたら、弊社カスタマーサポートまでお気軽にお問い合わせください。

今後とも、どうぞよろしくお願い申し上げます。

敬具

【三井住友カード】
カスタマーサポートチーム
[東京都江東区豊洲2丁目2番31号 SMBC豊洲ビル]

メール文面の例

出典：フィッシング対策協議会
「QR コードから誘導するフィッシング (2024/08/28)」
https://www.antiphishing.jp/news/alert/qr_20240828.html

2024年の事例：誘導文面の変化（ポイントプレゼント）

- 今まで多かった危機感をあおるような、セキュリティ向上、不正利用、本人確認などの文面よりも、ポイント付与の方が警戒がゆるむ？

実際に行われていたキャンペーンを模倣

過去のキャンペーンを模している？実際にありそうと思ってしまう

JCBで外食をもっとお得に！

毎月抽選で100人に5,000ポイント！

JCBカードをお持ちの方へ、Gurunaviで外出時のお得なキャンペーン！毎月抽選で100名様に**5,000ポイント**をプレゼントいたします。

確認するだけで簡単受け取り！必要な情報を確認するだけで、すぐに5,000ポイントをゲット！

簡単3ステップで完了：

1. 下記のボタンをクリック
2. ログインして基本情報を確認
3. その場でポイントを受け取る！

ポイントを今すぐ受け取る

※キャンペーンは期間限定ですので、今すぐお手続きください。

詳細やご利用条件については**こちら**をご確認ください。
このメールは送信専用です。ご質問がある場合は**こちら**よりお問い合わせください。
メール配信を停止する

今すぐ最大10,000円相当のPayPayポイントをゲット！

いつもPayPayをご利用いただき、ありがとうございます。

10月限定の特別キャンペーンで、**最大10,000円相当のPayPayポイント**が当たるチャンス！日常のお買い物や支払いで簡単に参加できます。

キャンペーン概要

2024年11月01日（金）～11月31日（土）

- **PayPayを使うだけ**で、自動的に抽選に参加。最大10,000円分のポイントが当たるチャンス！
- 便利店やレストランなど、日常生活のあらゆる場面でPayPayを使って、簡単に参加できます。
- 毎日お買い物をするたびに、チャンスが広がります。

今すぐ詳細を見る

ポイント付与方法

キャンペーン終了後、当選者にはPayPayアプリ内で通知されます。ポイントは11月中旬に付与されます。

注意事項

本キャンペーンは予告なく変更・終了する場合がございます。
付与されたポイントはPayPay残高にチャージされますが、出金はできません。

各種クレカブランドで同様の文面が報告されている

●●●●様

こんにちは、J-WESTカードより特別なお知らせです。

★ WESTERポイント 期間限定キャンペーン ★

2024年1月以降にJ-WESTカードをご利用いただいたお客様に、特別に10,000 WESTERポイント（1万円相当）をプレゼントいたします。このポイントは、ICOCAのチャージや鉄道のご利用、その他の特典にご利用いただけます。

さらに、J-WESTゴールドカード以上の会員様は1.5倍のポイントを受け取ることができます。

キャンペーン参加方法

以下のリンクをクリックして、今すぐお申し込みください。本キャンペーンは48時間以内にお申し込みが必要ですので、早めのご対応をお願いいたします。

▼[今すぐポイントを受け取る]
https://www-westjr.●●●●.com/?points=●●●●

■ ご注意事項：
[redacted] の部分のリンク
<https://www-westjr.●●●●.com/?points=●●●●> など

このキャンペーンはJ-WESTカード会員様のみが対象です。

すべてのポイントは15営業日以内にアカウントに自動的に反映されます。

何かご不明な点がございましたら、西日本旅客鉄道株式会社 カスタマーサービス（[redacted]）までお気軽にお問い合わせください。

＜お問い合わせ＞
西日本旅客鉄道株式会社
〒530-8341 大阪市北区梅田三丁目1番3号
[redacted]（ナビダイヤル）
営業時間: 月-金 9:00-18:00（土日祝休業）

JR West Co., Ltd. 2024

引き続き、J-WESTカードをご愛顧賜りますようお願い申し上げます

メール文面の例

出典：フィッシング対策協議会「WESTER をかたるフィッシング (2024/10/28)」
https://www.antiphishing.jp/news/alert/wester_20241028.html

2024年の事例：月額利用通知

■ 本物のメールと誤認するような文面でなりすまし

差出人　三井住友カード <info@smbc.co.jp>
件名　【三井住友カード】ご請求金額確定のご案内

なりすまし

SMBC 三井住友カード

※本メールは次回お支払いがあるお客さまに配信しています。

平素は三井住友カードをご利用いただき、誠にありがとうございます。次回のお支払い日についてご案内いたします

「お支払いについてのご案内」

お支払い日　7月4日（火）

ご利用明細のご確認はこちら ›

※Vpassへのログインが必要です

よく見ると「カード」のフィッシングなのに「銀行」のサイトに遷移、とある。しかし本物に雰囲気が似ており、受信者は気が付かない可能性がある

SMBC 三井住友カード

平素は三井住友カードをご利用いただき、誠にありがとうございます

※本メールは次回お支払いがあるお客さまに配信しています。

今月お支払い分の「リボ払い」「分割払い」へのご変更は31日23:59まで可能です。

今月のお支払い金額が多いと感じた方へ1回払いのお買い物も、「あとからリボ払い」「あとから分割払い」に変更することで今月のお支払い金額を減らすことができます。

「お支払い日についてのご案内」

お支払い日　**7月27日（金）**

※三井住友銀行のサイトへ遷移します※

詳細はこちら ›

Vpassへのログインが必要です

10月、フィッシングとして報告されたメール。本物？

SMBC 三井住友カード

ー大切なお客さまへのご案内ー

いつも当社のクレジットカードをご利用いただき、誠にありがとうございます。
今月のお引落日をご案内させていただきます。お引落口座へのご準備をお願い致します。

お引落日：2024年10月28日（月）

※ご案内が行き違いの場合はご容赦ください。

アプリ、ＷＥＢからご請求額の確認ができます！

アプリから確認

「Vpassアプリ」ならご請求額がひと目でご確認いただけます。
「Vpassアプリ」のダウンロードはこちら

Vpass　Vpassアプリ
生体認証で素早く安全にログイン

2024年の傾向：メールアドレスなりすまし送信の急増

- **5月ごろから、フィッシングの対象ブランドとは関係のない事業者のドメイン名になりすましたメール配信が急増**
- 特定のドメイン名のなりすましで、数百億通単位で大量に配信することもあれば、事業規模の大小を問わずドメイン名のなりすましで小規模に送信するケースもあった
- DMARCポリシーがnone、つまり認証失敗しても配信、という設定のドメイン名が中心となって使われていた
- DMARCポリシーがquarantine、つまり隔離する設定でも迷惑メールフォルダーへ配送されるため、受信者はそのドメイン名のブランドが迷惑メール送信者とみなされていた
- DMARCポリシーはreject、つまりドメイン名なりすましメールは排除する設定にしなければ、ドメイン名毀損に繋がっていくことがわかった

2024年10月調査用メールアドレスに届いたフィッシングメールの例

【重要なお知らせ】メルカリ事務局からのお知ら...	メルカリ <no-reply@accounts.nintendo.com>	2024/10/14 7:19
【アイフル株式会社】特別な利息無料キャンペ...	アイフル株式会社 <service@costcojapan.jp>	2024/10/14 10:18
【アイフル株式会社】特別な利息無料キャンペ...	アイフル株式会社 <info@costcojapan.jp>	2024/10/14 10:46
【重要なお知らせ】メルカリ事務局からのお知ら...	メルカリ <no-reply@accounts.nintendo.com>	2024/10/14 10:55
【重要】Amazonアカウントの情報更新をお届...	Amazon <bjxxzr@vpass.ne.jp>	2024/10/14 11:12
【重要なお知らせ】お客様のお支払い方法が承...	Amazon.co.jp <tonanpwn@vpass.ne.jp>	2024/10/14 11:18
Amazon.co.jp お客様のご注文がキャンセルさ...	Amazon.co.jp <amazon.co.jp-appagp.signin-o...	2024/10/14 11:29
【重要なお知らせ】メルカリ事務局からのお知ら...	メルカリ <no-reply@accounts.nintendo.com>	2024/10/14 11:55
Amazonプライム会費のお支払い方法に問題...	Amazon <pzmqnatfadr@costcojapan.jp>	2024/10/14 12:11
JCBカード利用制限解除のために手続きが必...	MyJCB（サイト・アプリ） <my.jcb.security.O3oma...	2024/10/14 13:54
【重要なお知らせ】メルカリ事務局からのお知ら...	メルカリ <no-reply@accounts.nintendo.com>	2024/10/14 15:29
【重要】Amazon.co.jp異常ログイン通知	Amazon.co.jp <wiqphtdp@costcojapan.jp>	2024/10/14 16:35
アカウントセキュリティ審査結果のお知らせ	MyJCB（サイト・アプリ） <my.jcb.security.N2nma...	2024/10/14 17:19
【楽天市場】アカウントの支払い方法を確認で...	【楽天市場】<pre_reg@ac.rakuten-bank.co.jp>	2024/10/14 17:59
[重要]：【お客様のプライム特典が現在利用で...	Amazon <hbokgrl@sbishinseibank.co.jp>	2024/10/14 18:08
10月限定！最大10,000円相当のPayPayポ...	Paypay <paypay-no-reply@costcojapan.jp>	2024/10/14 18:38
【Amazon 重要なお知らせ】あなたのAmazon...	Amazon <rkco@costcojapan.jp>	2024/10/14 18:52
[重要]：【お客様のプライム特典が現在利用で...	Amazon <pety@costcojapan.jp>	2024/10/14 18:59
【プロミス】5000Vポイントをすぐにお受け取りくだ...	p-mail <update@accounts.nintendo.com>	2024/10/14 19:31
【重要なお知らせ】AEON ご利用確認のお願い	AEON <order-update@aeon.co.jp>	2024/10/14 20:32
<MyJCBアカウントに関するご確認のお願い>	JCBカード <jcb-108z@costcojapan.jp>	2024/10/14 20:55
Amazon.co.jp お客様のご注文がキャンセルさ...	Amazon.co.jp <amzaon.co.jp-appagp.signin-o...	2024/10/15 2:38
お支払い予定金額のご案内 TS CUBIC CARD	MY TS CUBIC <toyats3club-ja.accont.userl-jan...	2024/10/15 2:48
<イベント番号：PM-77813350309-MyJCB...	JCBカード <myjcb-q4yF@costcojapan.jp>	2024/10/15 3:03
【重要なお知らせ】メルカリ事務局からのお知ら...	メルカリ <no-reply@accounts.nintendo.com>	2024/10/15 3:43

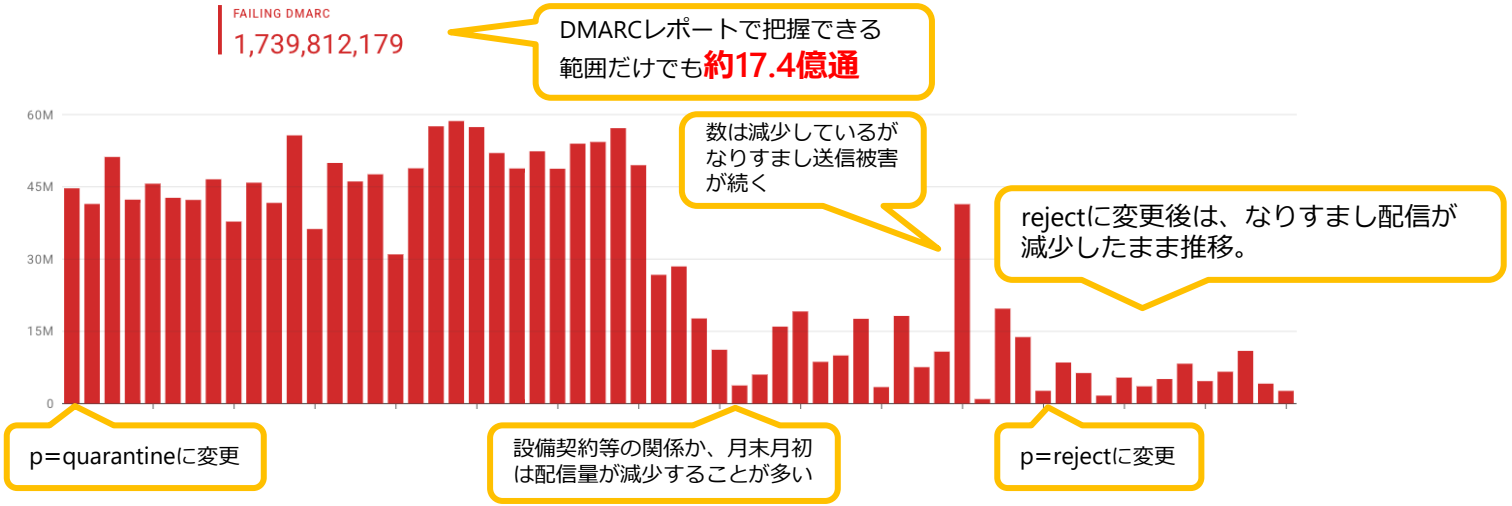
2024年の傾向：メールアドレスなりすまし送信の急増

■ なりすまし送信被害にあった事業者の被害状況（DMARCレポート集計）

- p=noneからquarantineにDMARCポリシーを変更したが、なりすまし送信は止まらなかった
- p=rejectに変更後、沈静化。なりすまし送信は続いたが、報告数が激減したため、着信しづらくなったと考えられる
- しかし、数カ月間、大量になりすまし送信されていたため、**ドメイン名=ブランドへの信頼性の低下**を招いた

なりすまし送信による被害：メルマガ経由での購買が減少
→ 利用者が正規メールも信用しなくなった

メールマーケティングを行っている
事業者にとっては大問題
落ちた信用はすぐには回復できない



2024年の傾向：フィッシングURLを大量生成

- ランダムサブドメイン＋独自ドメイン名でURLを大量生成
- ワイルドカードで登録されており、IPアドレスは同一＝同じサーバーに大量のURLが紐づいている

2024/9/3	11:40:43	ヤマト運輸	https://yvortfejzlxmtjmcjnt.znxtsc.cn/	未知	.21.30.46
2024/9/3	11:42:36	ヤマト運輸	https://acltxjcxnpcyfsqcfrgbxt.znxtsc.cn/	未知	.21.30.46
2024/9/5	15:37:17	ヤマト運輸	https://wdyjrxusqiqlalcrc.znxtsc.cn/caoni	未知	.21.30.46
2024/9/11	20:22:46	Amazon	https://wdvoohbhjyncvogfsksb.racist.cn/	未知	.21.2.86
2024/9/11	17:46:23	Amazon	https://tfpvdqvadgvbitsgkj.racist.cn/	未知	.21.2.86
2024/9/11	18:06:00	Amazon	https://rzbtwthqhdioqow.racist.cn/	未知	.21.2.86
2024/9/11	18:22:16	Amazon	https://glklhjiylunuea.racist.cn/	未知	.21.2.86
2024/9/12	14:27:50	Amazon	https://htxmkiqdywdyqmzbbilx.racist.cn/	未知	.21.2.86
2024/9/12	15:40:01	東京電力	https://qnoufgjlrluotfyhrjvfijhsi.zunhuaab	未知	.21.26.60
2024/9/12	17:23:52	東京電力	https://yfsvkotkcgpshb.zunhuaabc.cn/	未知	.21.26.60
2024/9/17	4:38:38	東京電力	https://zitgtbetrebpklxothikl.zunhuaabc.c	未知	.21.26.60
2024/9/18	6:34:37	東京電力	https://uondqmjfqxdhi.zgtpcda.cn/	未知	.21.21.221
2024/9/18	6:40:32	東京電力	https://ahnrgqisgjbknuqhenapo.zgtpcda.c	未知	.21.21.221
2024/9/18	6:53:14	東京電力	https://sbgyojltycfp.zgtpcda.cn/	未知	.21.21.221
2024/9/18	6:59:02	東京電力	https://hxiazqzgmbbnucj.zgtpcda.cn/	未知	.21.21.221

```
$ host *.dza[redacted].cn
*.dza[redacted].cn has address [redacted].[redacted].[redacted].26
```

ワイルドカード＝サブドメイン名をアスタリスク（*）で指定しても同じIPアドレスが返ってくる

この例では青枠がサブドメイン名、
ピンク枠がドメイン名

サブドメイン名　ドメイン名

https://rzbtwthqhdioqow.racist.cn/
https://glklhjiylunuea.racist.cn/

同じドメイン名でサブドメイン名が長さも文字列も違うものが多く、同じドメイン名のものはIPアドレスも同じだった

URLを大量生成する手法はここ数年続いているが、特に2024年は1回しか使わない「使い捨て」傾向が強かった。
フィルター回避やテイクダウンされづらくすることが目的と思われる。
ドメイン名単位でみると、同一のIPアドレスに誘導されるので、フィッシングに使われたドメイン名がワイルドカードで登録されていると確認できた場合は、ドメイン名ごとにフィルター登録等の処理が必要。

正規サービスを悪用する例

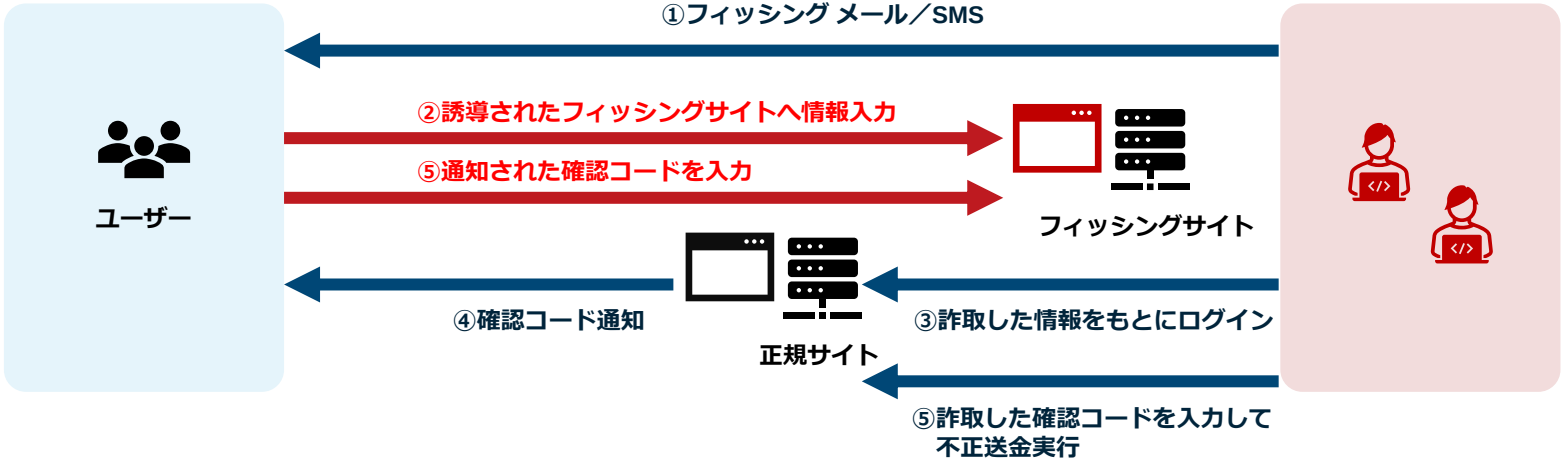
- フィッシングURL
  - 短縮URL、DDNSサービスを使用したフィッシング
  - Google翻訳を経由してフィッシングサイトへ誘導する手法
  - 特殊なIPアドレス表記を用いたURL

例）

- 短縮URL
  https://rebrand.ly/****
- DDNSサービス
  https://servicecssam86.duckdns.org/?*******
- Google翻訳経由
  https://translate.google.com/translate?sl=auto&tl=ja&hl=ja&u=https://ancient-feather-b86e.h0o8rowdum.*******.***/
  ※ページ翻訳機能へフィッシングURLを指定している
- IPアドレスに16進数や8進数等を使用
  http://●●●●.0xc0.154/
  http://●●●●.0x1c.071763/

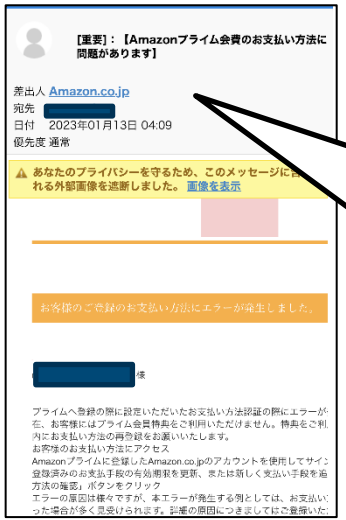
リアルタイムフィッシング

- 2段階認証（確認コード、ワンタイムパスワード等）を突破するために使用
- 不正送金被害増加の要因
- リアルタイムで情報を詐取しながら、バックグラウンドで正規サイトを操作



スマートフォンの普及による影響

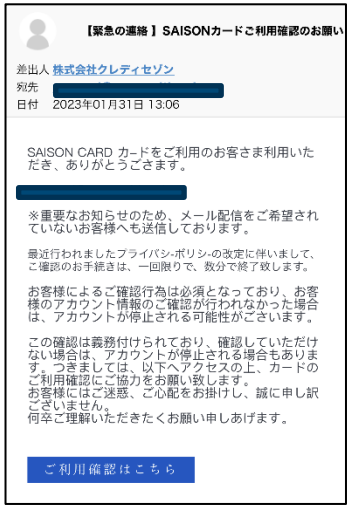
- 幅広い年齢層の方々がメールやインターネットサービスを活用
  - スマートフォンユーザーのセキュリティ意識の低さ
  - 狭いディスプレイ。見にくい小さい文字。省略化された文字表示
  - 本物のメールやWebサイトをコピーしたフィッシングに気付けない
  - SMSフィッシング（スミッシング）によるフィッシング



ディスプレイネームしか表示されない。長押しすると見える

Amazon.co.jp <news-amazon@rhsvlrv.cn>

赤文字：ディスプレイネーム
青文字：本当のメールアドレス



フィッシングメールなのに差出人メールアドレスが本物の場合も

なりすまし送信メール

メールアドレスを確認しても意味がない

フィッシング対策

フィッシング対策ガイドライン

フィッシングは世の中の状況にあわせて、常に変化し進化しているため、
毎年内容を精査し、改訂版を公開（最新版は2024年6月8日公開）

■改訂内容
使いやすさや読みやすさを向上させ、より役立つものになるように全体的な更新を行いました
◇ コンテンツへの動線の見直し。基本的な概念の説明や用語集を付録に移動
◇ 情勢の変化を受けた項目を削除
◇ 要件を示す内容とその実施方法を示す内容とを分別
◇ 付録にフィッシング対策チェックリストの追加

■ フィッシング対策ガイドライン

https://www.antiphishing.jp/report/guideline/antiphishing_guideline2024.html

Webサイト運営者向けの対策ガイドライン
フィッシング被害を未然に防ぐための注意点や、フィッシングが発生した場合の対応を、ガイドラインとして整理

■ 利用者向けフィッシング詐欺対策ガイドライン

https://www.antiphishing.jp/report/guideline/consumer_guideline2024.html

一般利用者（消費者）向けの対策ガイドライン
フィッシング事例を多く掲載し、インターネットサービスを利用する上での注意点や対策、被害に遭ってしまった場合の連絡先等を、ガイドラインとして整理

事業者の対策

フィッシング対策ガイドライン重要５項目

1. **利用者に送信するメールでは送信者を確認できるような送信ドメイン認証技術等を利用すること**
2. **利用者に送信するSMSにおいてはなりすましが起きにくいサービス（国内で直接接続される送信サービス）を利用し、発信者番号を利用者に告知すること**
3. **複数要素認証を要求すること**
4. **ドメイン名は自己ブランドと認識して管理し、利用者に周知すること**
5. **フィッシング詐欺について利用者に注意喚起すること**

出典：フィッシング対策協議会「フィッシング対策ガイドライン」https://www.antiphishing.jp/report/guideline/antiphishing_guideline2024.html

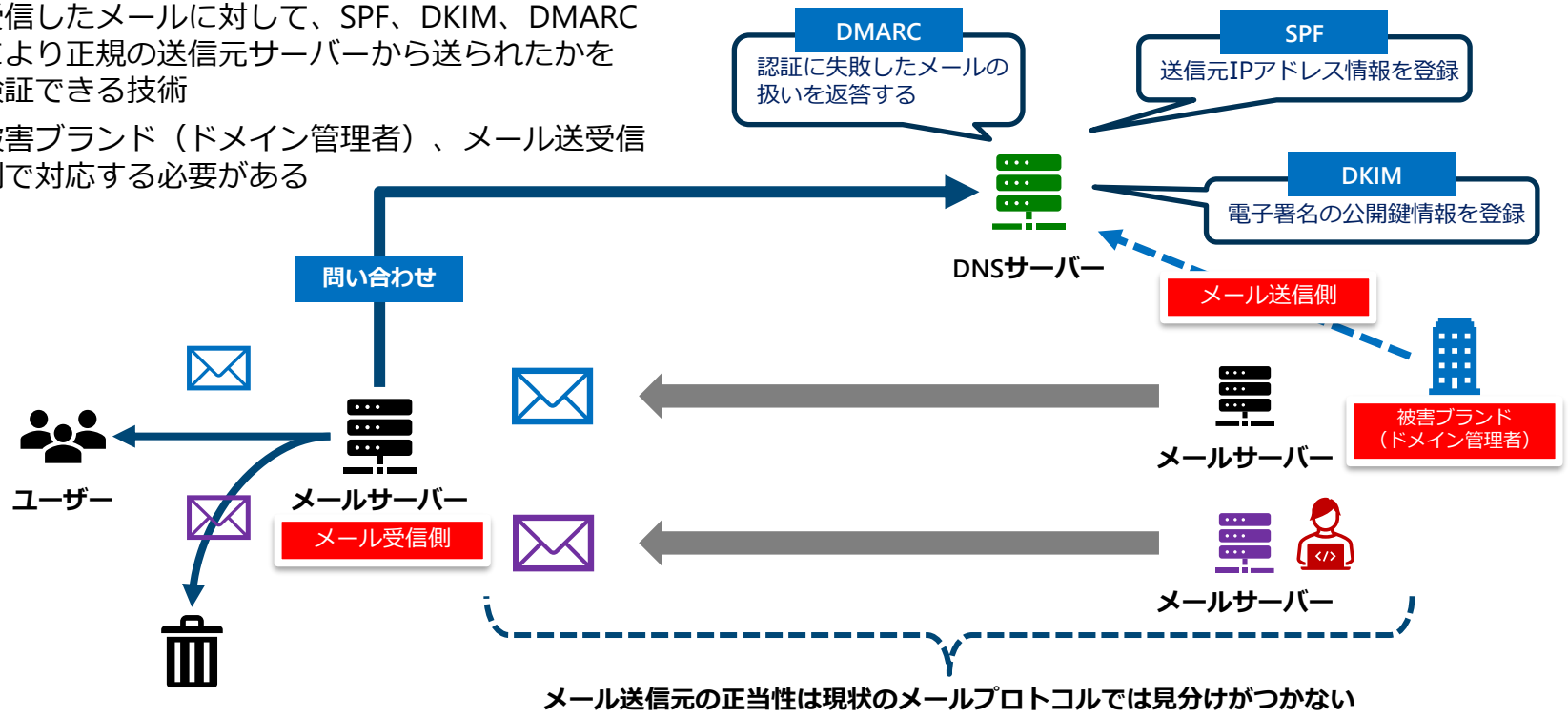
フィッシング詐欺対策 最重要項目

1. 利用者に送信するメールでは送信者を確認できるような送信ドメイン認証技術等を利用すること

4. ドメイン名は自己ブランドと認識して管理し、利用者に周知すること

なりすまし送信メール対策：送信ドメイン認証

- **正規ドメインの差出人メールアドレスで詐称したなりすまし送信メールに有効**
- 受信したメールに対して、SPF、DKIM、DMARCにより正規の送信元サーバーから送られたかを検証できる技術
- 被害ブランド（ドメイン管理者）、メール送受信側で対応する必要がある



送信ドメイン認証DMARCのメリット

送信ドメイン認証DMARC

- Gmailメール送信者ガイドラインで一括送信者（5,000通／日以上メールを送信する送信者）は対応が必須となったことで、日本国内でも普及が進んだ
- ドメイン名管理者はDMARCの認証に失敗（fail）したメールの扱いをポリシーとして指定できる
  - none：認証失敗（なりすましメール）してもそのまま素通しする
  - quarantine：認証失敗したら迷惑メールフォルダーへ配信
  - reject：認証失敗したら受信拒否（破棄）
- ドメイン名管理者はDMARC認証が成功（pass）したか失敗（fail）したか等のフィードバックレポートを受け取れる（レポート送信を行っているメールサービス：Gmail、マイクロソフト、NTTドコモなど）

送信ドメイン認証DMARCに対応するメリット

- 正規メールが届いているか、DMARCレポートで確認できる
- なりすましメールを配送しないよう指定できる（フィッシングメール、マルウェア添付メール等）
- DMARCで認証された正規メールにロゴを表示するBIMIやブランドアイコン等が利用できる
- 受信側はモバイルを中心に7割以上が対応済み
  Gmail（Androidスマートフォン標準）、 Apple iCloudメール（iPhone等Apple製品標準）、NTTドコモ、au/KDDIメール、ソフトバンク、楽天モバイル、Outlook.com、Yahoo!メール、各種メールセキュリティ製品

正規メールがフィッシングとして報告される

- **【重要・緊急】入出金を規制しました――“詐欺っぽい”三井住友銀行のメールが話題　一体なぜ？経緯を聞いた（Itmedia）** https://www.itmedia.co.jp/news/articles/2308/30/news163.html

「【重要・緊急】入出金を規制させていただきました…などのメールは詐欺です」――そんな件名のメールが話題になっている。一見すると詐欺メールのように見えるが、送り主は、本物の三井住友銀行だ。

- フィッシング対策協議会には、本物の注意喚起メールがフィッシングとして報告された

送信日時：2023年8月8日
差出人：三井住友銀行 <smbc_info@msg.smbc.co.jp>
件名：【重要】ショートメッセージ(SMS)の確認コードしか見ないのは大変危険です！
報告件数：**約21件**

送信日時：2023年8月30日
差出人：三井住友銀行 <smbc_info@msg.smbc.co.jp>
件名：【重要・緊急】入出金を規制させていただきました…などのメールは詐欺です
報告件数：**約22件**、件名に [meiwaku] が付加されたものは3件

いずれも
- S/MIME署名あり
- DMARC pass
- SPF/DKIM pass

正規メールとしては完璧な、申し分ないメール。しかし、受信者は正規メールかどうかを認識できていない

ここ数年、偽メールは見分けられない、と啓発してきたが、それでは正規メールも疑うしかない。利用者にメールを送る必要がある以上、「正規メールと証明されたメールがある」という啓発が必要。現状、啓発すべき点は以下の2点

・送信ドメイン認証によって正規メールと認証されたメールの見分け方を知ってもらう

・セキュアなメールサービスを利用してもらう

正規メール視認性向上の取り組み（BIMI）

- 利用者にとって必要なのは、正規メールかどうかの判断を助ける情報
- 長い文章で注意を書いても読まないし、判断が難しい

利用者にはこの情報だけで大事なことが十分に伝わる

2024年末時点ではGmail、Apple iCloudメール、au／KDDIメール等で対応済み

このゴールに向けてはDMARC正式運用（quarantineまたはreject）が必須

対応後

対応前

●●●●からお送りするメールの差出人の正しいドメインは@●●●●.co.jpです。
しかしメールアドレスを偽装した偽メールが送られる場合もあるので注意してください
また～かどうかも…

対応前　対応後

BIMI（Brand Indicators for Message Identification）：DMARCで認証された正規メールにブランドアイコンを表示する技術

送ったメール、利用者にはどう見えている？

■ 2024年11月、Gmailアプリでメールボックスを表示したら、BIMI対応ブランドが増えていた

メール本文を見ると惑わされるので、件名一覧で判断できる方が良い

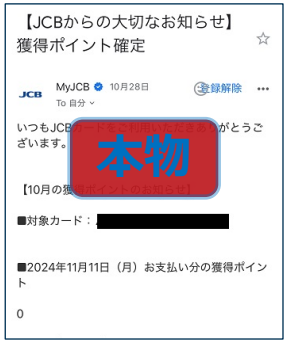
ブランドロゴが表示されていると、目立つし安心感を与える

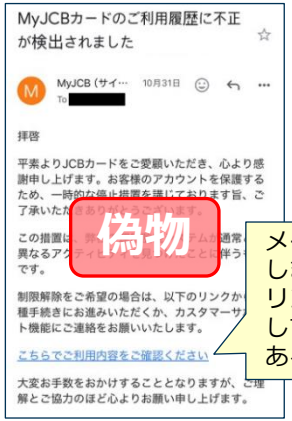
利用者にはこのロゴ表示の情報だけで大事なこと（このメールは安全）が十分に伝わる

**実は銀行からの正規メール
ロゴがないと目立たないし、
偽メールかもしれないと心配で、
メールを開こうという気持ちになれない**

S/MIMEで署名されているが、一覧やメール表示画面では確認できないのでメールを開く対象となりづらい

**MyJCBからのメール2件、ロゴありとロゴなし
メールを開かなくても、一覧表示の違いで気付くことができる**

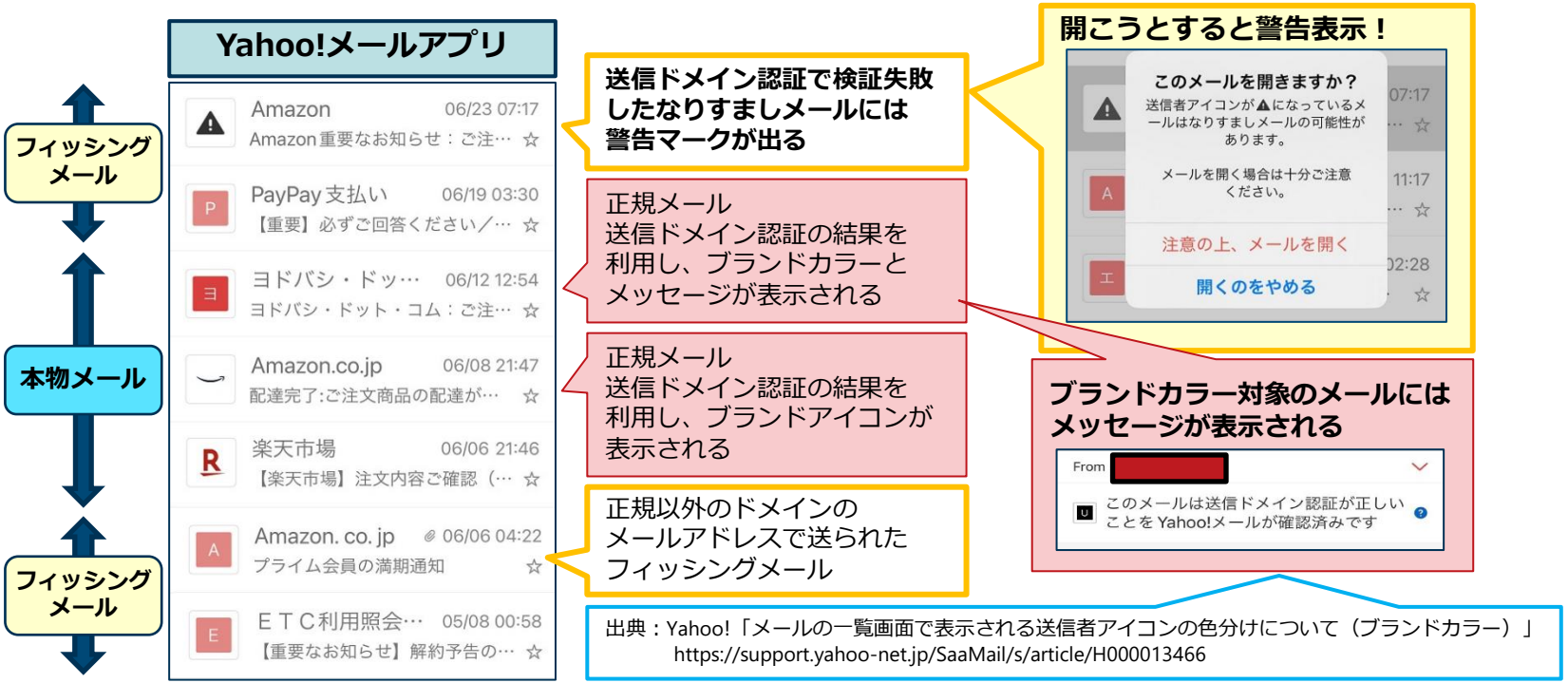




メール本文を見てしまうと惑わされ、リンクへアクセスしてしまう恐れがある

正規メール視認性向上の取り組み（Yahoo!メール）

- Yahoo!メールでは、送信ドメイン認証結果に応じて、警告表示等を行っている
- BIMIと似たサービスとして、ブランドアイコンというサービスも提供
  https://announcemail.yahoo.co.jp/brandicon_corp/



出典：Yahoo!「メールの一覧画面で表示される送信者アイコンの色分けについて（ブランドカラー）」
https://support.yahoo-net.jp/SaaMail/s/article/H000013466

なりすましメール対策（DMARC）関連資料

- 迷惑メール対策推進協議会：関連資料について
  https://www.dekyo.or.jp/soudan/aspc/report.html
  - 送信ドメイン認証技術導入マニュアル第3.1版
    https://www.dekyo.or.jp/soudan/data/anti_spam/meiwakumanual3/manual_3rd_edition.pdf
  - 送信ドメイン認証技術　DMARC導入ガイドライン
    https://www.dekyo.or.jp/soudan/data/anti_spam/dmarc_guideline.pdf

運用者向け
専門的で詳しい

- Google : Gmail
  - なりすまし、フィッシング、迷惑メールの防止を支援する
    https://support.google.com/a/topic/9061731?hl=ja
  - Google :BIMI を設定する
    https://support.google.com/a/answer/10911320?hl=ja

運用者向け
Googleのサービスでの設定方法が詳しく記載されているが、全体的な設定の流れや各技術の説明はわかりやすく、参考となる

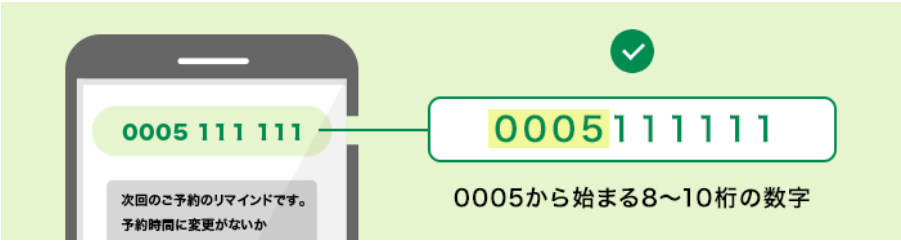
- なりすまし対策ポータル「ナリタイ」
  https://www.naritai.jp/

読みやすい
DMARCのことを知りたい方向け

- フィッシング対策協議会：なりすまし送信メール対策について
  https://www.antiphishing.jp/enterprise/domain_authentication.html

SMS送信元表示名 共通番号

- ドコモ、KDDI、ソフトバンク、楽天モバイルの携帯キャリア4社が企業単位で審査・発行する「0005」から始まる8～10桁の表示名
- 重複のない番号で**なりすまし防止**
- 携帯キャリア4社で共通の番号のため**正規メッセージを判別しやすい**



出典：NTTドコモ「共通ショートコード」https://www.docomo.ne.jp/service/sms/displayname/

認証強化（絵文字認証）

■ リアルタイムフィッシングによる被害

— SMSによる確認コード、ワンタイムパスワードも詐取

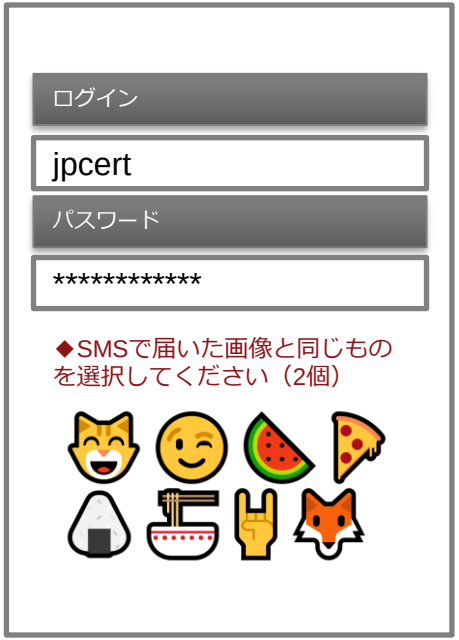
■ 絵文字認証

— ランダムに表示された絵文字から、SMSやメールで通知された絵文字（1～2個）を選択（入力より難易度が低い）

— ランダムに表示される絵文字は毎回変わり、偽サイトでの再現が難しい

— 偽サイト上で絵文字の選択ではなく入力を求められても、数千文字の中から入力させることは困難

— すでに確認コードを送信する機能を有するシステムの場合、実装難易度が低い



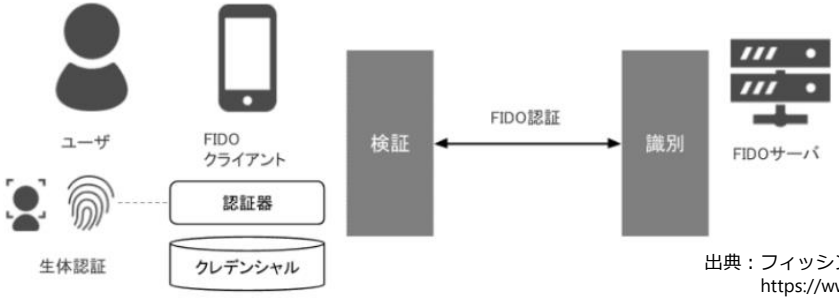
認証強化（パスキー）

これまでのクレジットカード情報の保護対策

- PCI-DSS準拠
- 加盟店サイトでは決済代行システムを利用　**フィッシング詐欺による不正ログイン**
- 3Dセキュアの普及　**リアルタイムフィッシングによる被害**

FIDO/Passkey

- 認証にパスワードを使用しないパスワードレスの技術
- パスキーと呼ばれるオンライン認証の仕組みで、スマートフォンなどの生体認証を使用して個人認証が可能
- 公開鍵方式を採用し、認証情報である秘密鍵が端末内で安全に管理され、セキュリティリスクを低減
- 正規ドメインでないサイトからのアクセスを防ぐことが可能となりパスワードに起因するフィッシング被害を防ぐ



出典：フィッシング対策協議会「フィッシングレポート2024」
https://www.antiphishing.jp/report/phishing_report_2024.pdf

認証強化と利便性向上

パスワードマネージャー

- パスワードや認証情報を管理するツール
- AndroidおよびiOSスマートフォン、PCで利用可能（アプリ、ブラウザー）
- 基本機能としては、ログインするサイトごとにIDとパスワードを登録する
- パスキー情報も管理可能となってきている

利用者側でのフィッシング対策の一つとしてぜひ推奨して欲しい

パスワードマネージャーを使うメリット

- 長く複雑なパスワードを設定しても覚えなくてよい
- 登録済みのサイトにはログインするが、偽（フィッシング）サイトには反応しない（気が付ける）

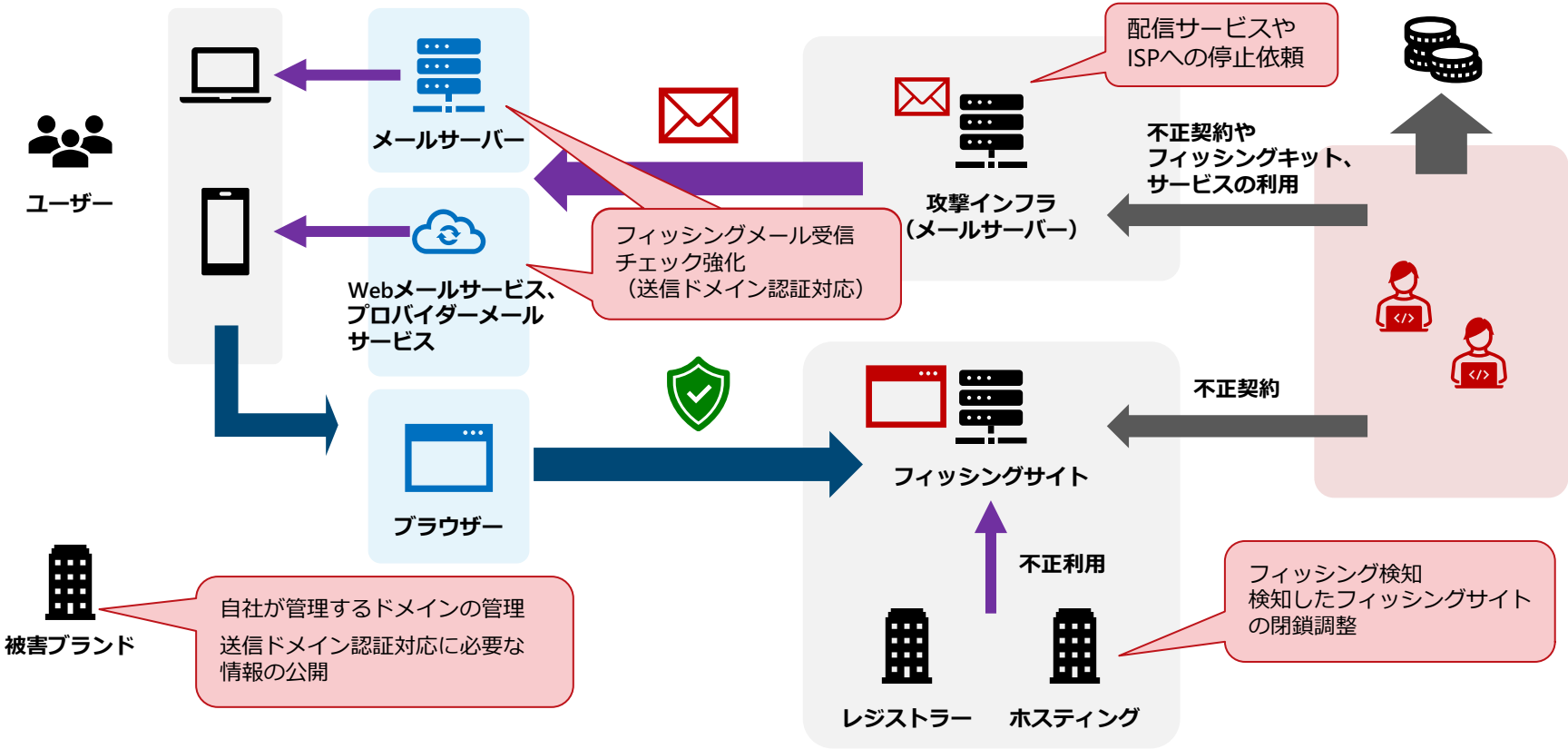
パスワードマネージャーを使う際の注意

- 認証強度は上がらない（パスワードの複雑さに依存）ので、安易なパスワードを利用し続ける危険がある
- IDとパスワードを調べて手動入力可能（偽サイトにログイン情報を手入力する危険性は残る）
- パスワードマネージャーおよびデバイス自体のセキュリティに配慮が必要（生体認証でロックする等）

サービス提供側の注意点

- サイト遷移のたびに何度もパスワードを聞かれるのは不安を感じるので、遷移することを表示して伝える

フィッシング詐欺への事業者対応



フィッシングサイト対応

- フィッシングサイトの検知
  - X（旧Twitter）等のSNSからの情報収集
  - ユーザーからの報告
  - 検知サービスの利用（テイクダウンを含む場合もある）（推奨）
- フィッシングサイトの閉鎖調整（テイクダウン）
  - ホスティング事業者等へのサイト閉鎖依頼
  - JPCERT/CCや該当事業者（推奨）が実施
- URLフィルタリング
  - フィッシングサイト閉鎖までの利用者保護のため
  - Google Safe Browsing等へのURL登録

検知サービスの活用

- 早期にURLフィルタリングへの登録、サイト閉鎖調整を行えるため、被害抑制に効果が期待できる
- 組織内に専門の人員や設備がなくても、迅速な対応が可能
- サービスによって検知手段に差異があり、分野も得手不得手があるため、事前検証は必要
- 2022年度版の「フィッシング対策ガイドライン」で検知サービスの利用を「必要に応じて」から「推奨」へ変更

フィッシング対策まとめ

なりすましメール対策はブランドとドメインを守るための基本的なセキュリティ対策と考える
　　送信ドメイン認証、正規メールの視認性向上

フィッシングサイトへの対応（発見、URLフィルター登録、テイクダウンなど）は、
早期に行うほど効果が高い。検知サービスの活用

フィッシング事例を収集し、自ブランドでの対応方法を検討しておく

一度フィッシングの標的になると、なりすましメール対策を完全に行わない限り、
狙われ続けることを認識する（対策をすると減る傾向あり）

自己紹介

一般社団法人JPCERTコーディネーションセンター
国内コーディネーショングループ リーダー、シニアアナリスト

吉岡 道明（よしおか みちあき）、CISSP

◆経歴

1993年　システム開発、情報セキュリティ会社 入社

システム開発事業部門にてSE/DBA/PMとして開発プロジェクトに従事
DBセキュリティ対策やDB監視システム開発支援に携わった後、2007年 データベースセキュリティ研究所の上級研究員として、セキュリティ事業部門に異動。インシデント対応支援、WAF導入支援などの業務に従事する傍ら、執筆や講演活動も行う。
2011年からは、セキュリティコンサルティング部門の部門長。
その後、セキュリティコンサルタントとして、インシデント対応支援、情報セキュリティアドバイザー、CSIRT構築支援などに従事

2018年　一般社団法人JPCERTコーディネーションセンター 着任（現職）

フィッシング対策協議会における、フィッシング報告受付業務、および事務局担当として従事する傍ら、執筆および講演活動を行っている

◆業界団体での活動

・フィッシング対策協議会 事務局長（2024年6月～）

◆講演活動

・Webセキュリティ、フィッシング詐欺に関するセミナー講演
　－セキュリティ・ワークショップ in 越後湯沢
　－千葉インターネット防犯協会
　－フィッシング対策セミナー（フィッシング対策協議会）
　－日本クレジット協会
　－埼玉県クレジットカード犯罪対策連絡協議会 など多数

◆執筆活動

・専門誌・サイトへの寄稿
　ーDBマガジン、gihyo.jp、bizgate など
・『情シス担当者のための絵で見てわかる情報セキュリティ（DB MagazineSELECTION）』（共著）

お問い合わせ、インシデント対応のご依頼は

JPCERTコーディネーションセンター

- Email：pr@jpcert.or.jp
- https://www.jpcert.or.jp/

インシデント報告

- Email：info@jpcert.or.jp
- https://www.jpcert.or.jp/form/

脆弱性に関するお問い合わせ

- Email：vultures@jpcert.or.jp
- https://jvn.jp/

ご清聴ありがとうございました